WHITE PAPER

SEPTEMBER 2002

TREND MICRO, INC.
10101 N. DE ANZA BLVD.
CUPERTINO, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
WWW.TRENDMICRO.COM

Trend Micro, Inc.
ROI for Antivirus Software and Services

TABLE OF CONTENTS

September 2002
Trend Micro, Inc.

Survey conducted by Gartner Consulting. This should not be deemed to be an endorsement by Gartner of any Trend Micro product or service. Gartner expressly disclaims all warranties, expressed or implied, of fitness of this material for a particular purpose. The results may vary from Gartner's published research position.

EXECUTIVE SUMMARY

Economic slowdown in the marketplace often manifests in greater rationalization for investments in information technology (IT). Companies may no longer base IT investment decisions on irrational "need to update/upgrade" thought processes, nor are they typically purchasing based on established relationships within their respective technology/vendor communities. In the current economic climate, most companies will increasingly base their IT purchasing decisions on the return on invested (ROI) funds. Essentially, companies are now looking for a demonstration of value for their investment.

In light of this need to demonstrate value, Trend Micro, Inc. (Trend Micro) commissioned a report to uncover the benefits and the ROI of its virus protection strategy. The report provides insight into the costs and benefits related to deploying the Trend Micro product line strategy at three tiers of virus protection, namely, gateway, server, and desktop levels.

Input gathered from eight different cross-sections of companies, spread out in various geographical regions of the world, indicates that there are significant benefits associated with deploying Trend Micro antivirus software and services. The areas where the most time and cost savings were identified are as follows:

- Reduced system downtime
- Faster assessment and cleanup of related system and application damage
- Efficient automatic distribution of signature upgrades and updates
- Effective virus monitoring activity
- Fewer resources spent in pre- and post-deployment testing procedures
- Less time spent on training and educating IT personnel on virus protection, and real location of IT employees to other areas
- Ease of integration and deployment due to Trend Micro's compatibility with legacy systems.

Each of the components identified were rolled up to calculate the following range for both ROI and payback period respectively.

The ROI calculated from the data captured from a diverse set of industries ranged from 19 to 67 percent.

The payback period ranged from 6 to 10 months.

The ROI and payback period proved to be very favorable for all eight of the interview locations. Although many factors contributed to the cost-reducing and revenue-enhancing benefits of Trend Micro, downtime, damage assessment, and cleanup proved to be the most important factors that have a bearing on ROI. In addition, companies with fewer mission-critical operations face less expensive repercussions from a virus infection, while higher ROIs resulted from companies with more mission-critical operations.

Downtime decreased as a result of a reduction in the number of viruses infiltrating the system and upgrade/update test costs were reduced as a result of both confidence in Trend Micro testing procedures and Trend Micro's efficient method of disseminating the upgrades/updates. Having a more proactive, accurate, and updated scan for viruses has led to reduction of the resources required for damage assessment and cleanup. Lastly, the ability to monitor, assess and clean up viruses at remote locations from a centralized location reduced the travel costs associated with employees assigned to manage virus protection in their organizations.

INTRODUCTION

Escalating enterprise costs and the issues associated with controlling software vulnerabilities have begun to trigger change in the security status quo. Successful enterprise information software security requires finding the appropriate balance between containing the risks that come with new technology developments and enabling the benefits to enterprises and end users resulting from its use. Despite the pains and costs associated with trying to add security after applications and systems have been developed or procured, security remains largely an afterthought. However, enterprises that must deal with continual requirements are starting to evaluate and re-evaluate whether their current approaches toward security are adequate.

1

Although the debate regarding the responsibility for quality and security software is not new, the issue has taken on increasing importance as the direct and indirect costs of poor software security continues to increase in enterprises.[1]

1. Software Security: Change Is Imminent," 10 June 2002, Arabella Hallawell, Gartner Analyst.

INFORMATION SECURITY SPENDING TRENDS

According to recent surveys, information security budgets average between three percent and five percent of overall IT budgets; some industry budgets vary outside this range. This doesn't include additional spending on information security by business units that choose to boost security beyond the protection offered by central IS organization.[2]

2. Safety First for Information Security Solutions," 14 June 2002, Vic Wheatmen and Arabella Hallawell, Gartner Analyst.

"Another report states that

- Cyber-incidents nearly doubled in 2001, and are expected to double again in 2002.
- Decreased financial losses experienced during the first material attack will offset the costs of building a security-aware enterprise."[3]

3. Building a Security-Aware Enterprise: Companies Forces," 17 January 2002, Rich Mogull, Gartner Analyst.

"Until recently, enterprise antivirus was frequently dismissed as a saturated and increasingly commoditized market. However, viruses continue to be the biggest security challenge for enterprises, and they account for a large portion of enterprise spending on security.

"During the same period, however, the virus risk changed substantially. Viruses are created more frequently and can infect enterprises at a rapid rate, often before a software update is available from the antivirus vendor, and before the enterprise can distribute the update to relevant platforms. The need for continual updating already has enterprises buckling under the costs and effort involved."

"The mature enterprise antivirus market is poised to undergo significant upheaval during the next two years. However, attention to the basics of antivirus products—product and service quality, and management functionality—will position vendors most successfully for the pending market transition."[4]

4 . Expect Turmoil in the Antivirus Market," 22 May 2002, Arabella Hallawell, Gartner Analyst.

The current economic, business and technology climate has created many business discontinuities and changes in market behavior as the confidence in the economy has weakened. To some vendors, these pressures feel like bad news, and to vendors with foresight, this can be extremely good news. Trend Micro is a visionary company with a strong presence in the arena of antivirus software and services. Given the existing economic environment, Trend Micro wants to seize the market opportunity by shifting its focus from mere innovation in product technology to improvement in business processes that manifest in greater market penetration. The genesis of this study can be traced back to Trend Micro's desire to present compelling quantitative and qualitative reasons to facilitate enterprises' decision-making process to invest in its antivirus software and services.

OBJECTIVES

Trend Micro commissioned a third-party company to evaluate the ROI of its antivirus software and services. The salient objectives of this study are as follows:

- To identify the components to evaluate the ROI of antivirus software and services
- To understand the cost, benefit, and investment considerations of enterprises deploying antivirus software and services
- To uncover the relationship and impact of a virus protection software investment on a cost-and-benefits basis.

KEY FINDINGS

MARKET DYNAMICS

Prevention is always preferable to searching for a cure. Some of the recent virus attacks have shown that, at an absolute minimum, enterprises cannot afford to leave their virus protection strategies fragmented. Enterprises should have the goal of providing virus detection tools on all levels of virus entry; namely, gateway, server, and desktop. Defining and following virus protection strategies involves not just the enterprise, but also the virus protection supplier and third parties to minimize vulnerability.

Variations in policy and in policy language and management, which occur when tools from different antivirus suppliers are used, may require manual reconciliation. Regular and frequent

update processes are critical. As such, enterprises should view virus protection as a strategy wherein the technology and processes used should account for different user needs, fit with existing management systems, and be subject to change-management standards.

Historically, most enterprises have not had a single antivirus supplier and they have been readily prepared to switch among them. This is corroborated by the data points collected as a part of this study. However, centralized and coordinated risk management is becoming increasingly important to help enterprises manage and contain explosive virus outbreak costs. As such, Trend Micro facilitates centralized virus management. In addition to this, the real-time information that Trend Micro disseminates to mitigate the risk of viruses helps companies to gain greater business and technology efficiency. This enables enterprises to harness the power of a scarce and quantifiable element, "elapsed time." Deploying antivirus software and services by the same vendor, at each layer, facilitates the reduction of this elapsed time and extends the reach of enterprises horizontally across the whole enterprise. It also extends the reach of information vertically to cycles of activity in every layer of the enterprise network.

Most enterprises using Trend Micro antivirus software and services have an added benefit of transitioning to Trend Micro's enterprise protection strategy (EPS). Trend Micro EPS helps enterprises to build a robust, scalable, and standards-based foundation that supports a true plug-and-play enterprise security architecture.

PROFILE OF COMPANIES INTERVIEWED

The enterprises contacted in this study are either evaluating or re-evaluating their virus protection strategies or have recently organized in a way to ensure that virus risk is managed effectively on all three tiers. The extent and the specific strategies for virus protection vary from company to company, depending on the size of the organization and its culture. However, most of the companies are managing viruses centrally.

The companies interviewed were spread out across different geographical areas of the world. One of the companies is located in Australia, one in Singapore, two have head offices in Europe, and the remaining four are located in the United States. The revenue of these companies ranged from US$100 million to US$42 billion. The number of users ranged from 500 to 200,000, and in most cases, more than 90 percent of users were based in the corporate headquarters. The companies spanned various sectors, such as educational, government, high technology, and electronic components manufacturing. Most of these companies have been Trend Micro customers for at least one year, and one company in particular has been a Trend Micro customer for more than six years.

COSTS AND BENEFITS OF VIRUS PROTECTION

The ROI calculations undertaken in this study take a one-year time horizon into consideration. This presents a fairly conservative yet realistic view of ROI. Seven key components of Trend Micro's antivirus software and services have been identified that have an explicit cost-saving or revenue-enhancing benefit associated with them. If one were to measure and include the soft cost benefits, the ROI will be higher. Some of the factors that constitute these soft costs are as follows:

- Company reputation for responsible business practices and sound IT operations
- Greater security of invaluable customer, supplier, and employee data
- Protecting a company's intellectual capital and content
- Fostering long-term relations and creating goodwill with customers, suppliers, and employees
- Reduced employee stress due to the reduction of the threat of a virus attack
- Employee work-life balance.

As stated above, most of the companies interviewed utilized Trend Micro's antivirus software and services at all three tiers of virus protection; namely, gateway, server, and desktop levels. The main reason each company chose a three-tiered approach is due to the evolving methods of virus infiltration experienced over the last few years.

Gateway and server protection was viewed as a priority in every company, due to the infiltration of viruses via the network and executable email files. Although the number of viruses that infiltrated each company after the introduction of Trend Micro was reduced drastically, the most common method of infiltration before and after the introduction of Trend Micro's software and services was at the gateway and desktop levels. Five out of the eight interviewees estimated that up to 60 percent of viruses entered their environment via the same method over and over again.

Business processes most frequently affected by virus infiltration are manufacturing operations, email, financial transactions, business-to-business (B2B) and business-to-consumer (B2C) transactions. No instances of critical data loss were recorded because all the companies had instituted efficient and effective backup strategies and practices.

Figure 1.
Key Components that Affect ROI for a Trend Micro's Antivirus Software and Services

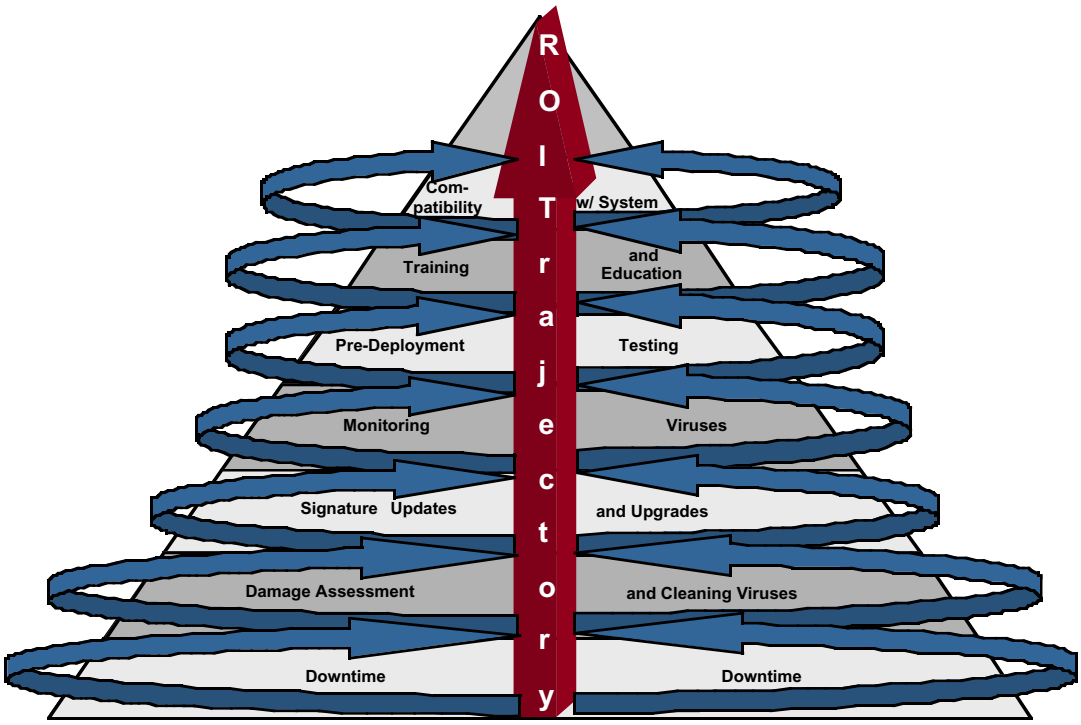

Figure 1 depicts the components identified in this study that have a significant impact on ROI. Each component cascades into the other component to contribute in building the ROI trajectory for an enterprise investing in Trend Micro's antivirus software and services.

The following is a discussion of these components and their impact on ROI.

DOWNTIME

In most cases, downtime is the most important measure to gauge the degree of virus damage. Though downtime has an industry accepted definition, in common parlance downtime is understood as either a complete system shutdown or a major slowdown that affects a business unit negatively. The severity of downtime is magnified if a company's operations are mission-critical, such as materials tracking system in a manufacturing environment. Therefore, the damage and loss due to downtime varies depending on the mission-criticality of companies operations.

Prior to the introduction of Trend Micro's antivirus software and services, companies experienced between 60 to 200 hours per year of downtime due to virus infections. After the introduction of Trend Micro, the number of hours of downtime was reduced significantly

to about 0 to 40 hours per year. The average cost of virus-related downtime after the introduction of Trend Micro ranged from US$100 to US$10,000/hour.

DAMAGE ASSESSMENT AND CLEAN-UP

Virus infiltration at the server and gateway are the most complex and difficult to assess for damage and cleanup costs; desktops are usually the most expensive to completely clean up, because of the number of desktops in an enterprise and also as a source of virus infection. In some cases, a virus may have to be removed on a desktop-to-desktop basis. For companies with thousands of these devices, this cost can prove to be an extremely expensive proposition. The interviewees estimated that the cost to assess and clean a system after a virus incident ranged from US$500 to US$10,000 before the introduction of Trend Micro to US$0 to US$3,600 after the introduction of Trend Micro. One company estimated that virus assessment and clean up took on average three full-time employees over three days to complete a full clean-up, at a cost of approximately US$3,000.

SIGNATURE UPGRADES AND UPDATES

In most cases prior to using Trend Micro, signature upgrades and updates were not disseminated automatically, and the manual upgrade/update process was time consuming and required extensive testing. Although testing is still conducted by seven of the eight companies interviewed, the duration, and hence the cost, of testing has been greatly reduced due to confidence in Trend Micro's product and automatic distribution of virus-related information. The cost to download, install and test each upgrade/update on a per-company basis was reduced from a broad range of US$400 to US$5,000 to a more narrow range of US$0 to US$400 per upgrade/update.

MONITORING VIRUS ACTIVITY

Since most enterprises are viewing virus protection as a strategy, there has been a shift from a reactive to a proactive approach to stemming virus infiltration into their organization. Monitoring virus-related activity is becoming increasingly important. The average time spent monitoring viruses ranged from four to 1,000 hours per year prior to Trend Micro and one to 52 hours after. The average cost per hour to monitor viruses ranged from US$35 to US$200 per hour.

PRE- AND POST-DEPLOYMENT TESTING

Prior to deploying Trend Micro's antivirus software and services, it was common for each company to hire contract engineers for pre-deployment testing, updating pattern files and ongoing virus protection integration costs. After the introduction of Trend Micro's software and services, most companies were satisfied with the testing procedures adopted and

instituted by Trend Micro, and the procedures enabled them to reallocate or greatly reduce the number of engineers and contract engineers assigned to virus protection. The total costs ranged from US$11,000 to US$56,000 before the introduction of Trend Micro and US$0 to US$3,000 after the introduction of Trend Micro.

INTEGRATION WITH LEGACY SYSTEMS

Most of the interviewees stated that they had not experienced integration incompatibility issues with the existing legacy systems while running Trend Micro's software and services. In this instance, significant information for before-and-after scenarios was not captured due to the lack of accurately captured data. One interviewee estimated that the cost to integrate past and present virus protection strategies into their legacy systems was approximately US$10,000. The cost to uninstall and reinstall a three-tier virus protection strategy was reduced with the introduction of Trend Micro. These costs ranged from US$1,000 to US$20,000 before companies deployed Trend Micro and US$0 to US$2,000 after the introduction of Trend Micro's software and services.

TRAINING AND EDUCATION

Three types of possible training programs related to virus protection were identified for the user, help desk and IT personnel (IT also includes employees dedicated to virus protection). Most companies rarely offer end-user and help-desk training related to viruses. Although IT departments did offer training to the employees responsible for virus monitoring, damage assessment and clean up, these costs were relatively low both before and after the introduction of Trend Micro. In two instances, training averaged approximately four days per year at a cost of approximately US$450 per day prior to the introduction of Trend Micro. After the introduction of Trend Micro, the interviewees estimated that these costs were cut in half, due to the user friendliness of the product and the support provided by Trend Micro's technical services department.

TRAVEL

Travel to and from headquarters to remote locations prior to and after the introduction of Trend Micro's antivirus software and services was not a major issue, due to the centralized location of most hardware and the availability of local personnel or contractors. One interviewee estimated that prior to the introduction of Trend Micro software and services, approximately 12 travel days were required to address remote virus issues. Since the introduction of Trend Micro, most companies felt comfortable with the remote access to all sites and systems from the corporate location, and in many cases travel was greatly reduced or eliminated altogether. Although interviewees were unable to quantify the costs, most interviewees felt that there were savings realized by reducing the need for outside contractors to service remote locations in the event of a virus outbreak.

The following table lists the key component contribution to the ROI for Trend Micro's antivirus software and services.

Table 1.
Key Components Contribution to ROI for Trend Micro's Antivirus Software and Services

Components	Before the Introduction of Trend Micro	After the Introduction of Trend Micro
Downtime	60-200 hours/year	0-40 hours/year
Damage assessment and cleaning viruses	US$500-10,000/incident 120-400 incidents/year	US$0-3,600/incident 0-10 incidents per year
Signature upgrades and updates	US$400-5,000 upgrade/update	US$0-400 per upgrade/update
Monitoring virus activity Pre- and post-deployment testing	4-1,000 hours/year US$11,000-56,000/year	1-52 hours/year US$0-36,000/year
Training and education Integration with legacy systems	0-4 days/year US$1,000-20,000/year	0-2 days/year US$0-2,000/year

Overall, these cost savings along the outbreak life cycle can be broken down into two distinct areas: operations and efficiency. Operational costs, such as downtime, allow the company to maintain critical operations related to the revenue stream of the company. These costs can be high for companies that have greater reliance on their IT infrastructure. The efficiency introduced by Trend Micro helps to effectively mitigate virus-related problems and ensures that there are significant cost savings and quantifiable benefits associated with deploying its antivirus software and services. For instance, less time is needed for damage assessment, upgrades/updates, clean up, etc., which allows a company to possibly reallocate the staff dedicated to virus protection, and in some cases, reduce the contractors located at corporate or remote locations to address virus-related problems.

ROI AND PAYBACK PERIOD

CALCULATION

ROI entails isolating and adding the net cost-reducing and revenue-enhancing benefits introduced by Trend Micro's product and then dividing this sum by the total investment. For the purposes of this study, the time period investigated was a 12-month (one-year) period, as opposed to an ROI calculated through to the obsolescence horizon of the product. Performing a one-year ROI allows for a conservative calculation of the ROI and payback period. There will probably be more benefits and cost savings realized over a longer time horizon, hence the ROI calculated might be higher.

The payback period is essentially a ratio and proportion calculation that compares all of the financial benefits realized in one year against the time in months it would take to

have that investment returned (e.g., financial benefits/one year = investment/X years, then solve for X). Although each payback period proved to be less than one year, as in the case with the ROI calculations, focusing on more than one year's worth of data would have reduced this period of time.

The investment estimate included all of the costs involved in licensing, deploying, debugging, and maintaining Trend Micro's antivirus software and services, though this estimate did not include any indirect, soft, or overhead costs involved in implementing them. In most cases, the indirect and soft costs would either be negligible or too difficult to quantify, while the overhead costs would be consistent regardless of the virus protection strategy implemented. In some cases, actual invoices were used to identify the investment figure, while in other cases a per-user charge along with a multiplier for all first-year fixed costs was used.

ROI AND PAYBACK PERIOD RANGE

The ROI calculated from the data collected from multiple industries identified above ranged from 19.2 percent to 67.3 percent. The company responsible for the lower range calculation of 19.2 percent realized a much lower downtime, damage assessment and clean-up benefit, due to the fact that a slowdown or shutdown of the IT environment was not as critical as all the other industries studied. The higher range ROI calculations were from companies where downtime, damage assessment and clean up were very expensive. Due to their critical need for uptime, these companies also spent more on testing upgrades/updates prior to the introduction of Trend Micro antivirus software and services.

The payback period ranged from 6.67 to 10.07 months. The low end of the payback period corresponds with the high end of the ROI calculation, while the higher end of the payback period corresponds with the lower ROI. Since a payback period calculates when the entire investment is returned, the higher the return, the faster—and therefore the shorter—the payback period.

Overall, both the ROI and payback periods calculated above represent very positive and realistic numbers. Although reasonable business efforts were utilized to uncover an exhaustive list of the financial benefits associated with Trend Micro's antivirus software and services, it is unreasonable to suggest that all benefits have been identified. It is safe to assume that there are most likely additional benefits that have not been identified before and after the initial questionnaire was developed, hence the ROI and payback period could be even more favorable than illustrated here.

CONCLUSIONS

The key areas of savings and improvement realized after the introduction of Trend Micro's antivirus software and services are as follows:

- Reduced downtime
- Faster assessment and clean-up of related damage
- Efficient automatic distribution of signature upgrades and updates
- Effective virus monitoring activity
- Fewer resources spent in pre- and post-deployment testing procedures
- Less time spent on training and educating IT personnel on virus protection and reallocation of IT employees to other areas
- Ease of integration and deployment because of compatibility with legacy systems.

The ROI range of 19 percent to 67 percent, calculated over one year for these eight different companies representing eight different industries, proved to be a very favorable investment. The payback period varies from six to ten months, also very favorable, and would allow enterprises to assign a complete payback to the product in less than one year for all eight of the companies studied.

Given this backdrop, enterprises must take into account the significant ROI and fast payback of Trend Micro's antivirus software and services prior to making their virus-protection buying decision. Enterprises should invest in virus protection strategy aggressively, because of the increasing sophistication of virus threats, and to avoid becoming marginalized or eliminated due to lagging technological capabilities.

METHODOLOGY

DEFINITIONS

ROI: The financial gain or loss expressed as a percentage of funds invested to generate that gain or loss. In other words, ROI is the net return realized by the introduction of a product or service. This is calculated as the net present value (NPV)/investment. NPV compares the value of a dollar today versus the value of the same dollar in the future after taking inflation and return into account.

For a given use of money in an enterprise, the ROI is how much "return," usually profit or cost savings, results. An ROI calculation is sometimes used along with other approaches to develop a business case for a given investment. If an enterprise has immediate objectives of getting market revenue share, building infrastructure, positioning itself for sale or other objectives, an ROI might be measured in terms of meeting one or more of these objectives rather than in immediate profit or cost savings.

Payback Period: The length of time required to recover the cost of an investment. This is calculated as the cost of project/solution divided by the annual cash flows. All other things being equal, the better investment is one with the shorter payback period.

QUESTIONNAIRE DESIGN

Figure 2 depicts the review of secondary research from various sources, which formed the foundation for designing the questionnaire. An interactive and collaborative process between a group of third-party analysts, third-party consultants, and Trend Micro personnel was adopted to develop the questionnaire for this study. The underlying objective of each question was to identify measurable qualitative and quantitative costs incurred and benefits realized by deploying antivirus software and services. The final questionnaire comprised of 34 questions and included a section to garner company-specific information.

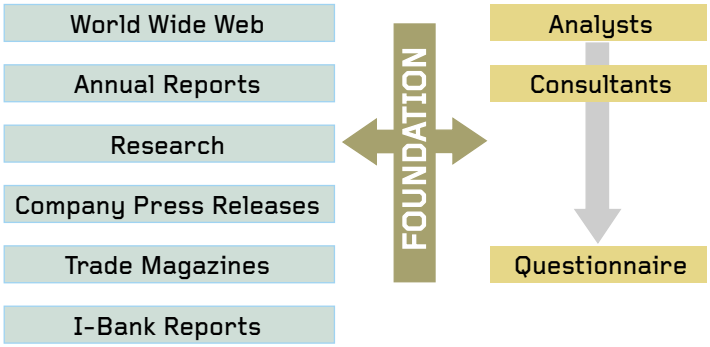

Figure 2.
Questionnaire Design Process

DATA COLLECTION

A total of eight interviews were conducted. The questionnaire was administered to collect data from the following two scenarios:

- Before a company deployed Trend Micro antivirus software and services at the gateway, server and/or desktop level
- After a company deployed Trend Micro antivirus software and services at the gateway, server and/or desktop level.

The questionnaire was administered during a one-hour telephone interview. All of the interviewees were manager level or higher and all worked within the IT security departments of their respective companies. In a few instances, respondents were unable or unwilling to answer some questions because they did not actually know the answer or they thought they would be divulging proprietary information.

DATA ANALYSIS

Upon completion of data collection, the information was reviewed for accuracy and consistency. Spreadsheets were created to separate the qualitative and quantitative data and categorize it into the before and after scenarios. The qualitative data was examined to extract the overarching non-quantitative benefits received from antivirus products across the cross-section of companies interviewed. The quantitative data was then analyzed for cost and revenue changes realized after the introduction of Trend Micro. For example, if downtime due to viruses were reduced from US$1 million to US$100,000 after the introduction of Trend Micro, a saving of US$900,000 would contribute to the overall ROI calculation.

Data consistency was maintained across a veritable melange of companies, because all the companies interviewed utilized Trend Micro products at the gateway, server, and desktop levels of virus protection. Despite this fact, in two instances, geographical concerns and established relationships with Trend Micro's competitor motivated two smaller remote offices to use competitive products at the desktop level; however, they had an insignificant impact on the ROI uncovered.

ABOUT TREND MICRO

Trend Micro provides centrally controlled server-based virus protection and content filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop.

Trend Micro's corporate headquarters is located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters is located in Cupertino, CA. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and service providers. Evaluation copies of all of Trend Micro's products may be downloaded from its award-winning Web site, http://www.trendmicro.com/.